MATHEMATICS OF COMPUTATION
Volume 66, Number 219, July 1997, Pages 1347–1351
S 0025-5718(97)00851-X

THE DIOPHANTINE EQUATION $x^4 + 1 = Dy^2$

J. H. E. COHN

ABSTRACT. An effective method is derived for solving the equation of the title in positive integers x and y for given D completely, and is carried out for all $D < 100000$. If D is of the form $m^4 + 1$, then there is the solution $x = m$, $y = 1$; in the above range, except for $D = 70258$ with solution $x = 261$, $y = 257$, there are no other solutions.

Over fifty years ago, Ljunggren [2], showed that the equation of the title, where without loss of generality D is square free, has at most one solution in positive integers. The method was purely algebraic, but rather complicated. It is the object of this note to provide an effective computational method of determining whether a solution exists and of finding it when it does.

Clearly, there can be no solution unless the equation $v^2 - Du^2 = -1$ has solutions, and in particular $q \equiv 1 \pmod 4$ for every odd prime factor q of D. Let $\alpha = a + b\sqrt{D}$ be its fundamental solution, and define $\beta = a - b\sqrt{D}$, and

$$u_n = \frac{\alpha^n - \beta^n}{2\sqrt{D}}; \quad v_n = \frac{\alpha^n + \beta^n}{2}. \tag{1}$$

Then for the equation of title we have for some odd m, $x^2 = v_m$ and $y = u_m$. Since $b | u_m$ we see that for any odd prime factor q of Db, $(x^2 \pm 1)^2 \equiv \pm 2x^2 \pmod q$ and so $q \equiv 1 \pmod 8$. Since D was assumed square free and clearly b must be odd, we see that $b \equiv 1 \pmod 8$. If D is odd, then $D \equiv 1 \pmod 8$, and so $4|a$ whence $D \equiv 1 \pmod{16}$. So we have two cases:

Case 1. $D \equiv 1 \pmod{16}$, every factor of D is congruent to 1 modulo 8;

Case 2. $D \equiv 2 \pmod{16}$, every odd factor of D is congruent to 1 modulo 8.

In Case 1 we find $4|a$ and in Case 2 $a \equiv \pm 1 \pmod 8$.

Theorem 1. *Let $a = AB^2$ where A is square free. Then $m = A$ provides the only possible solution.*

Proof. Since $\alpha + \beta = 2a$, $\alpha\beta = -1$, the sequence $\{v_n\}$ satisfies the recurrence

$$v_{n+2} = 2av_{n+1} + v_n \tag{2}$$

with initial values $v_0 = 1$ and $v_1 = a$.

For n odd, let $w_n = v_n/a$, which is also an integer. Then by (2) $w_{n+4} - w_{n+2} = 2v_{n+3}$, $w_{n+2} - w_n = 2v_{n+1}$. Thus

$$w_{n+4} - 2w_{n+2} + w_n = 2(v_{n+3} - v_{n+1}) = 4av_{n+2} \equiv 0 \pmod{4a},$$

Received by the editor March 4, 1996.
1991 *Mathematics Subject Classification.* Primary 11D25.

and so since $w_1 = 1$, $w_3 = 3 \pmod{4a}$, it follows that for all odd n

$$w_n \equiv n \pmod{4a}. \tag{3}$$

In particular, solutions are possible only if $a = 2^{2\alpha}a_1$ where $\alpha \geq 0$ and a_1 is odd. In this case, we have for all odd n with $(a, n) = 1$

$$(w_n|a_1) = (n|a_1) = (a_1|n)\xi = (a|n)\xi, \tag{4}$$

where $\xi = -1$ if $n \equiv a_1 \equiv 3 \pmod 4$ and $\xi = 1$ otherwise.

Next we prove by induction on nN that for all odd coprime integers n, N the Legendre-Jacobi symbol $(w_n|w_N) = (n|N)$. This holds if $nN = 1$; suppose it is true for all values less than the one we consider. As n and N are supposed coprime, $n = N$ is impossible unless $n = N = 1$; without loss of generality we may assume $n > N$, since by (3) quadratic reciprocity gives $(w_n|w_N) = (w_N|w_n)\theta$, where $\theta = -1$ if $n \equiv N \equiv 3 \pmod 4$ and $\theta = 1$ otherwise. Then it is easily found that $w_n \equiv w_{n-2N} \pmod{w_N}$, and again $n - 2N$ and N are coprime. If here $n - 2N$ is positive, then $(w_n|w_N) = (w_{n-2N}|w_N) = (n - 2N|N) = (n|N)$ and the induction is complete; on the other hand if $n - 2N$ is negative, then we use $w_{n-2N} = -w_{2N-n}$ and then

$$(w_n|w_N) = (w_{n-2N}|w_N) = (-w_{2N-n}|w_N) = (-1|w_N)((2N - n)|N) = (n|N)$$

in view of (3), since if $N < n < 2N$, then $0 < 2N - n < N$.

Suppose that $x^2 = v_m = aw_m$; let n denote any odd integer coprime to am. Then

$$1 = (aw_m|w_n) = (a|w_n)(m|n) = (a_1|w_n)(m|n) = (w_n|a_1)(m|n)\xi = (am|n),$$

by (3) and (4) and this implies that am must be a perfect square, since otherwise, we may choose n to be congruent to 1 modulo 4 and also be a quadratic non-residue modulo am. Thus Am must be a perfect square, and to complete the proof we need to show that m cannot have any squared factor.

If $m \neq 1$, then m has an odd prime factor p, say $m = pk$, where $k \geq 1$. Then $v_m + u_m\sqrt{D} = \alpha^{kp} = (v_k + u_k\sqrt{D})^p$ and so

$$x^2 = v_k \sum_{r=0}^{\frac{1}{2}(p-1)} \binom{p}{2r} v_k^{p-2r-1} D^r u_k^{2r} = v_k \sum_{r=0}^{\frac{1}{2}(p-1)} \binom{p}{2r} v_k^{p-2r-1}(v_k^2 + 1)^r = v_k V,$$

say, where $V \equiv p \pmod{v_k^2}$. Thus we must have either $v_k = x_1^2, V = x_2^2$ or $v_k = px_1^2$, $V = px_2^2$. The former is impossible by Ljunggren's result.

Suppose then that $v_k = px_1^2$. We show that $p \nmid k$. For if $k = pK$, then we obtain as above $px_1^2 = v_{pK} = v_K V'$, say, where now $V' \equiv p \pmod{v_K^2}$. Since $p|v_K V'$ it follows that $p \| V'$ and hence that $v_K = x_3^2$, again impossible by Ljunggren's result.

This concludes the proof. □

For a given D it is therefore in principle trivial to solve the equation; all that is required is to determine a, calculate v_A and test whether it is a square. Unfortunately there are a number of practical difficulties occasioned by the huge values that occur; for example, when $D = 97441$, a has 289 decimal digits. Since the determination of A is nearly of the same order of difficulty as a complete factorisation of a, we consider how the calculations can be reduced.

The first step in the computation for any $D \equiv 1$ or $2 \pmod{16}$ is to eliminate any that are squares or have an odd prime factor $\not\equiv 1 \pmod 8$, and then to calculate

the continued fraction of $\sqrt{D}$ up to the end of the first period. There is a very efficient algorithm for doing this involving only integer arithmetic. If the period length is even, as occurs for example for $D = 34$, then the equation $v^2 - Du^2 = -1$ has no solutions, and so the equation of the title has none. Assuming the period length n to be odd, if $\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{n-1}, 2a_0}]$, we next calculate the convergent a/b corresponding to $[a_0, a_1, \ldots, a_{n-1}]$ which provides the fundamental solution α of $v^2 - Du^2 = -1$, as is well known. Provided multiprecision is available, this too can be carried out very efficiently. If here b has a factor congruent to 5 modulo 8 again there will be no solution; this occurs for example with $D = 193$ for which $b = 126985$, but it is not always feasible to use this unless b has a small such factor; it is not worth attempting a complete factorisation of b in other cases, as will become apparent.

As we have seen, a solution is possible only if $x^2 = v_A$, or equivalently if $w_A = AX^2$. Often, although it is impracticable to factorise a completely, we are able to find some of the factors of A. The following result is therefore of assistance.

Theorem 2. *A solution can exist only if for every factor k of A, $w_k = kX_1^2$, and in Case 2, every factor of A must be congruent to* $\pm 1 \pmod 8$.

For if $A = kl$, then as above

$$x^2 = v_k \sum_{r=0}^{\frac{1}{2}(l-1)} \binom{l}{2r} v_k^{l-2r-1} D^r u_k^{2r} = v_k \sum_{r=0}^{\frac{1}{2}(l-1)} \binom{l}{2r} v_k^{l-2r-1} (v_k^2 + 1)^r = v_k V$$

and again $V \equiv l \pmod{v_k^2}$. But now $l|a|v_k$ and so $v_k = lx_1^2$, $V = lx_2^2$, and so since $A = kl$ is square free, $w_k = lx_1^2/AB^2 = kX_1^2$.

In Case 2 we have that a and so also x and v_k are odd, and so modulo 8,

$$l \equiv V \equiv 1 + 2\binom{l}{2} + 4\binom{l}{4} = 1 + l(l-1) + \tfrac{1}{6}l(l-1)(l-2)(l-3),$$

whence $l \equiv \pm 1 \pmod 8$.

Theorem 3. *There is no solution if* $3|A$.

For as above, this would yield with $A = 3k$, $v_k = 3x_1^2$, $3x_2^2 = 4v_k^2 + 3$, and then $x_2^2 = 12x_1^4 + 1$. An easy descent argument shows that this equation is impossible, for it would require $x_2 \pm 1 = 2x_3^4$, $x_2 \mp 1 = 6x_4^4$ whence $\pm 1 = x_3^4 - 3x_4^4$. Here the lower sign is rejected modulo 3, and the upper sign requires x_3 odd and x_4 even. Thus $(x_3^2+1)(x_3^2-1) = 48(\frac{1}{2}x_4)^4$ and since $(x_3^2+1, 48) = 2$, we obtain $x_3^2+1 = 2x_5^4$, $x_3^2 - 1 = 24x_6^4$ and so $x_5^4 = 12x_6^4 + 1$.

Theorem 4. *There is no solution if* $5|A$.

For, it would give $v_k = 5x_1^2$, $5x_2^2 = 16v_k^4 + 20v_k^2 + 5$ with $x_1 \neq 0$, where $A = 5k$. Thus $4x_2^2 = 5(40x_1^4 + 1)^2 - 1$, whence $2(40x_1^4 + 1) = F_{3r}$, where $\{F_n\}$ denotes the Fibonacci sequence, and r is odd. To show that this cannot occur, let $\{L_n\}$ denote the Lucas sequence. Using standard identities for these sequences, we find it would require

$$80x_1^4 = F_{3r} - F_3 = \begin{cases} F_{6m}L_{6m+3} & \text{if } r = 4m+1 \equiv 1 \pmod 4, \\ F_{6m}L_{6m-3} & \text{if } r = 4m-1 \equiv 3 \pmod 4. \end{cases}$$

Now none of the Lucas numbers is divisible by 5, and since $(F_{6m}, L_{6m\pm3}) = 4$ we see that we require $L_{6m\pm3}$ to be a square or twice a square. By [1], this occurs only for $6m \pm 3 = 3$. The lower sign gives no value, and the upper gives only $x_1 = 0$.

Theorem 5. *If $3 \nmid a$, then $p \equiv \pm1$ or $\pm5 \pmod{24}$ for every factor p of A.*

For if $A = pk$, then $v_k \equiv a \pmod 3$ and we now have

$$px_2^2 \equiv \sum_{r=0}^{\frac{1}{2}(p-1)} \binom{p}{2r} a^{p-2r-1}(a^2+1)^r \equiv \sum_{r=0}^{\frac{1}{2}(p-1)} \binom{p}{2r} (-1)^r \pmod 3$$
$$= \frac{(1+i)^p + (1-i)^p}{2} = 2^{\frac{p}{2}} \cos\frac{p\pi}{4},$$

whence the result.

Theorem 6. *If $5 \nmid a$, then $p \equiv \pm1 \pmod 5$ for every factor p of A.*

For now we cannot have $a^2 \equiv 4 \pmod 5$ since $5 \nmid Db$. Thus $a^2 \equiv 1 \pmod 5$ and then $A \equiv \pm1 \pmod 5$. If $A = pk$ we must have $v_k = px_1^2$, and then $p \equiv \pm2 \pmod 5$ would give $v_k \equiv \pm2 \pmod 5$, since it is easily found that $5 \nmid v_k$, and then

$$px_2^2 = \sum_{r=0}^{\frac{1}{2}(p-1)} \binom{p}{2r} v_k^{p-2r-1}(v_k^2+1)^r \equiv \pm1 \pmod 5,$$

which is impossible.

We therefore tested whether a was a square; if so the problem is solved affirmatively. If not, then we attempt to eliminate D as simply as possible, by attempting factorisations of a, to find A, and of b. This may be difficult, but even when complete factorisations are impracticable, it may be possible to find enough information, for example if b has any factor $\equiv 5 \pmod 8$, or if A is divisible by 2 or 3 or 5, or if B is not divisible by 3 but A has a prime factor $\equiv \pm7$ or $\pm11 \pmod{24}$ or if B is not divisible by 5 but A has a prime factor $\equiv \pm2 \pmod 5$. If this fails to dismiss D, then we have to test for $v_A = x^2$. Even if A is known, the numbers are often far too large for a direct demonstration, and we use congruences. Let q denote any prime; then modulo q the sequence $\{v_n\}$ is periodic, and with period $z = z(q)$, say, not exceeding q^2. Then if $r \equiv A \pmod z, v_A$ could be a square only if the congruence $v_r \equiv x^2 \pmod q$ were soluble. It is usually quite easy to find a suitable q for which this fails to hold. If A is unknown but some of its factors are, then we use Theorem 2 instead and test for $w_k = kX_1^2$ in the same way.

To obtain a flavour of the work involved, when $D = 7393$, a is a number of 58 decimal digits, not divisible by 5 but having the unrepeated factor 13; thus this case can be eliminated by Theorem 6. When $D = 47858$, $a = 3719$, $b = 17$ and since 3719 is prime, we must consider ν_{3719}. We find that v_{3719} is not a square, since if $q = 11$, $z = 24$ and then $v_{3719} \equiv 10 \pmod{11}$. Not all values of D succumbed quite so easily.

All the solutions we have found arise from $A = 1$; we conjecture that this is always the case, although we are unable to prove it. [The equation $x^4 - 1 = Dy^2$ is more amenable to treatment along these lines.] A proof would eliminate much of the computation, for then all that would be required would be to test whether a is a perfect square. As we have seen, if $A > 1$ is a solution, then $w_k = kX_1^2$ for every factor k of A, and we know that we cannot have $k = 3$ or 5. We accordingly make the stronger

Conjecture. *The equation $w_k = kX_1^2$ is satisfied for no odd $k > 1$ and $a > 0$.*

For our purposes it would suffice to prove this for all odd *prime* k dividing A.

References

1. J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. **7** (1965), 24–28. MR **31:**2202
2. Wilhelm Ljunggren, *Einige Sätze über unbestimmte Gleichungen von der Form $Ax^4 + Bx^2 + C = Dy^2$*, Vid-Akad. Skr. Norske Oslo **1942** No. 9.

Department of Mathematics, Royal Holloway University of London, Egham, Surrey TW20 0EX, United Kingdom

E-mail address: j.cohn@rhbnc.ac.uk